Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

631.92.3

Berlin, 05 August 2020

535.1000
A56ID 75410
CR 126887
DD 126889
FD 142710

Final Decision

1. Facts concerning the data breach

- **Controller:** AWIN AG
- **Incident**: Credential stuffing (see bullet point 2)
- **Date of occurrence**: 08.07.2019
- **Date of acknowledgement of the incident**: 10.07.2019
- **EU/EEA Member States concerned, with the number of data subjects concerned**:
  - Ireland: 7 organisations
  - Italy: 3 data subjects
  - Spain: 4 data subjects
  - United Kingdom: 23 organisations
- **Category of data subjects**: customers (publishers)
- **Category of the data types/data records concerned**: First name, last name, address, email address, and bank account details of data subjects; name and email address of organisations
- **Likely consequences of the violation of the protection of personal data**: misuse of data

2. Description of the data breach from a technical-organizational perspective

An attacker used a stolen list of user names - typically email addresses and passwords - to try to gain access to the systems. Typically, these lists contain millions of email and password combinations.

This type of attack, known as credential stuffing, is based on people reusing the same username (typically an email address) and password on many different systems and Web sites.

On the night of July 8, 2019, an attacker used a leased botnet (a network of hacked computers or servers typically under the control of a hacker or criminals) to automatically send many thousands of requests to systems from about 100 different IP addresses. During this attack, the attacker could then match some of the stolen credentials with those on the systems.

The attack was logged in the systems, but did not generate any warnings or trigger any of the defence mechanisms. The activity was noticed on July 9, 2019, but was originally attributed to a known bug in the publisher login

Berlin Commissioner for Data Protection and Freedom of Information

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to disabled members of the public.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form for registering data protection complaints:
www.datenschutz-berlin.de/beschwerde.html

For all other enquiries, please send an e-mail to:
mailbox@privacy.de

Fingerprint of our PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to Kochstraße / Bus number M29 and 248

Visit our Website

https://privacy.de

process, which is occasionally exploited by attackers to bypass a registration fee.

3. Description and analysis of the effectiveness of the measures taken to address the personal data breach or to mitigate its adverse effects (Art. 33 (3) (d) GDPR)

The passwords of the affected accounts have been reset. A check for changes to the affected accounts was performed and these were reset if necessary. Improved detection and prevention of brute force attacks has been implemented and multi-factor authentication for platform user logins is under active development.

The password reset of the affected accounts prevented further consequences (redirection of payments was mentioned).

The detection and prevention of brute force attacks is inevitably only possible to a limited extent. As described above, the attacker has also invested a great deal of effort. Although the improvement of the corresponding measures is to be welcomed, it will only make future attacks more difficult.

The attack described is not due to a security leak, but to the fundamental weakness of knowledge-based authentication methods such as user name/password. It is therefore to be welcomed that the platform will introduce multi-factor authentication (e.g. adding the factor possession, such as TAN generators). However, given the limited amount and type of personal data accessible per account, we could not demand this at present (weighing of interests).

The implementation of multi-factor authentication prevents the success of the attack that has taken place.

4. Communication to the data subjects concerned or public communication (Art. 34(1) or Art. 34(3) (c) GDPR)

The controller has notified all data subjects and organisations concerned on 12 July 2019 via email about the incident.

5. Technical and organisational security measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

No particular measures beyond the standard IT security measures.

6. Subsequent measures by which the controller has ensured that a high risk to the data subjects concerned is no longer likely to materialise (Article 34 (3) (b) GDPR)

See bullet point 3.

7. Intended measures by the LSA Berlin DPA

7.1 Intended measures regarding Articles 33, 34 GDPR

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA closes the case.

7.2 Intended measures regarding data protection violations beyond Articles 33, 34 GDPR

Furthermore, the Berlin DPA has also not identified any data protection violations beyond Articles 33, 34 GDPR.

The problem lies with the users (publishers) who have used compromised passwords more than once. At best, the attack detection could be criticized. However, the high effort that the attackers have put in must be taken into account, which makes detection considerably more difficult. The violation would be considered minor at best. In addition, the possibility of a future attack will be closed by introducing multi-factor authentication.